Security and Emergency Plans

(Internal Policies)

Presented by We R

Team members:

Amwaj Alshamrani
Hassan Alibrahim
Khulud Alawaji
Latifah Alhwiseen
Mariam Alhawiti

Internal Policies

General Policies That Applied on All We R Systems

1. **General Policies**
    - The Data should be up to date (renewing training data)
    - Make sure the date & time are set correctly
    - Check all systems regularly and maintain it
    - Create structured policies for document retention and storage based on local, state, and federal requirements.

2. **Reporting a Security Breach**
    - Any member of staff who suspects that a theft, breach, or exposure of We R data has occurred must immediately inform the information security department.
    - Depending on the nature of the breached data, the information security department will determine whether the local law enforcement should be contacted to report the case.
    - If the security breach is done by one of We R employees, the process of removing all access to that employee will begin immediately and employee get fired.
    - If the stolen data has been published to the public (website, newspaper), We R will take the necessary action to remove the data immediately and employee too.
    - Data leak is NOT acceptable in any case and whoever is responsible for that leak will get fired immediately.

3. **Handling Client Information**
    - Data security to prevent loss and unauthorized access or use of the data during all stages (collection, processing, transmission, and storage).
    - customers data will be stored within Saudi Arabia and the local laws and regulations are applicable to the data.
    - We R will retain the client information for a period as minimum as it deems necessary to fulfil the purposes, unless applicable law requires a longer retention period.

4. **Internal Systems and Access**
    - Access to systems will only be provided to users based on business requirements, job function or responsibilities.

- All changes, and deletions to individual system access must be approved by the appropriate supervisor with a valid business justification.
- On an annual basis, We R will audit all user and administrative access for sensitive data.
- Discrepancies in access will be reported to the appropriate supervisor in the responsible unit and remediated accordingly.
- Administrators will immediately revoke all a user's access when a change in employment status, job function, or responsibilities dictate the user no longer requires this access.
- All remote access will be accomplished through of two factor authentication; a username and password or PIN combination, and a second method not based on user credentials, such as a certificate or token, provisioned to the user.
- Any third party that requires remote access to the systems for support, maintenance or administrative reasons must designate a person to be the Point of Contact (POC) for their organization. In the event the POC changes, the third party must designate a new POC.
- Third parties may access only the systems that they support or maintain.

5. Email and Internet Usage Guidelines

- Internet usage and emails will be subject to monitoring, which could occur at any time.
- Cannot send emails in a way that discriminates against anyone in any manner, including using language or other content that disparages groups based on age, race, colour, religion, gender, disability, or physical appearance.
- Employee must not receive email or newsletters from private companies for personal use, personal causes, or purchases unrelated to company business.
- Employee must not download software, including music, without consulting the supervisor, so that spyware and viruses aren't transferred to the computer network.
- Employee must not commit piracy, violate copyrights, discuss religion or politics, or use the internet for any lawful purposes

Specific Policies for Each Systems

1. **Advanced Surveillance System**

1.1. CCTV

- Ensure we don't capture more footage than we need to achieve our purpose in using the system.
- Ensure the security of the footage we capture – in other words, holding it securely and making sure nobody can watch it without good reason.
- Only keep the footage for as long as we need it – delete it regularly, and when it is no longer needed.
- Position our CCTV cameras for minimal intrusion, e.g. avoiding a private property (home window).
- Using privacy masking (Privacy masking is technology that 'blanks' out sensitive areas on a recording).
- Do not record conversations between members of the public.
- Do not install CCTV in traditionally private places, such as toilets.
- Do not share any CCTV recordings publicly e.g. on social media sites.
- Keep recordings secure and restrict access to them.
- Make sure you have enough recording space.

1.2. Facial Recognition

- Setting a minimum reliability and accuracy of the algorithm used.
- Retention duration of the photo used.
- Setting the auditing process of this criteria.
- Ensuring the faces dataset is inclusive and revised.
- Identify the limitation of the algorithm.

.

1.3. Gunshot Detection

- The sensor will record high frequencies where gunshot could be detected.
- Evaluate the accuracy of the gunshot sensor.
- Evaluate the accuracy given individual circumstances (ex. background noise)
- Timestamp should be recorded when the sensor identifies a gunshot.
- Protorirse gunshot alert.
- Integrate gunshot sensors with CCTV.
- Test the gunshot sensor for false detection (building and demolition)
- Built in maintenance functionally.
- Tampering alert.
- Heartbeat: gunshot sensor should have the ability to send a heartbeat signal to the control system to prove it is online and operational.

2. Counter Terrorism Airport (CTA)

2.1. X-Ray Scanning

- Each monitoring system connected to the scanner must have dual processors for increased computing power.
- Each monitoring system connected to the scanner must have high memory capacity for image scanning and image buffering.
- The Monitoring System screen must not be visible for passengers.
- If the scanner picks up a chemical or explosive item, the security officer cannot open the bag and wait for an explosive expert to attend the scene.

2.2. Ramming Prevention System

- Facial Recognition policies are applied.
- Scanning results should not be visible for other passengers.
- If the scan result is positive, the gate operator cannot open the gate. However, when the responding unit arrives at the scene they can open the gate if they find out the scan result is false.

2.3. Unattended Luggage

- Upon detecting an unattended luggage, the security team cannot open the luggage and search it without the passenger's consent.
- Each detected unattended luggage must have the duration and the location and passenger information if possible and be sent to the responding unit.

3. Energy Blackout Prevention System

- Access to consumers consumption data should be masked for control center and service providers.
- Access requests to consumers' sensitive data should be monitored and evaluated.
- When a consumer reports an issue or maintenance, the responding team must respond within ten minutes.

4. Fire System

- Fire employees have the permission to access the customer’s information and fire incident details.
- Evaluate the accuracy of the fire sensor.
- Test the fire sensor for false detection (building and demolition).

- Heartbeat: each fire sensor and water sprinkler sensor should have the ability to send a heartbeat signal to the control system to prove it is online and operational.